24-Stunden-Überwachung für Schul-IT

Nach dem Mega-Datenklau erhöht das Erziehungsdepartement das Sicherheitslevel.

Benjamin Wieland

Es war ein Diebstahl der gröberen Sorte. Insgesamt 1.2 Terabyte an Daten erbeuteten Kriminelle bei einem Angriff im Januar auf einen Dateiserver des Basler Erziehungsdepartements (ED). Stundenpläne, Absenzen, Telefonlisten, Adressen landeten im Darknet, aber auch private Hypothekarverträge und schulpsychologische Abklärungen.

Nun, neun Monate danach, gibt die Informatik des Basler Erziehungsdepartements weitere Details bekannt, wie sie solche Attacken in Zukunft verhindert will. «Wir planen die breite Einführung der Zwei-Faktor-Authentifizierung», sagt Thomas Wenk, Leiter Digitalisierung und Informatik Basel-Stadt. Bei dieser Massnahme ist jedoch noch nicht klar, ob und wie die jüngsten Nutzerinnen und Nutzer die Aufgabe meistern könnten.

Das Problem: Künftig müssten alle, die sich in ihr Edubs-Konto einloggen wollen, zwei Sicherheitsprüfungen überstehen. Notwendig wäre es dann also nicht nur, den Nutzernamen und das Passwort einzugeben, sondern zusätzlich einen Code. Den generiert eine spezielle App oder ein kleines Hardwaregerät.

Bei Banken normal, für Primarschulen nicht

Gerade bei Banken ist die Zwei-Faktor-Identifizierung mittlerweile gang und gäbe. Nur: Ein grosser Teil der rund 40 000 Nutzerinnen und Nutzer des Edubs-Netzwerks sind Minderjährige. Eine Zehnjährige könnte mit der Aufgabe überfordert sein, innert weniger Sekunden eine mehrstellige Ziffernfolge einzugeben.

«Wir sind daran, ein Konzept auszuarbeiten», sagt Thomas Wenk. «Bei den Jüngeren muss die Zweifach-Authentifizierung über die bestehende Infrastruktur funktionieren, nicht über ein mobiles Endgerät.» Man sei daran, sagt Wenk, zu eruieren, welche alternativen Anmeldeformen geeignet seien. Die rund 70 Mitarbeitenden der IT des Basler Erziehungsdepartements würden

> «Es kam bis heute nicht zu einer Kommunikation mit der Täterschaft.»
>
> **Thomas Wenk**
> Leiter Digitalisierung und Informatik Basel-Stadt

sich bereits mit der Zwei-Faktor-Authentifizierung anmelden.

Eine weitere Massnahme hatte das ED bereits im August bekannt gegeben. Neu sind E-Mails, die von ausserhalb der Organisation verschickt wurden, mit «Extern» vermerkt. Die Userinnen und User wissen dann: Im Zweifelsfall Links besser nicht anklicken und Anhänge nur mit grosser Vorsicht öffnen. Beim Angriff vom Januar geht man immer noch davon aus, dass die Erstinfektion über eine manipulierte E-Mail erfolgt ist. Von 761 Personen erbeuteten die Hacker Daten.

Von anderen Massnahmen haben die Schülerinnen, Lehrer und Sekretariatsangestellten meist aber nichts mitgekriegt. Die IT des ED lässt neuerdings den Datenstrom im System überwachen. Alarm auslösen kann etwa, wenn jemand versucht, via eine ausländische IP-Adresse auf das Mailkonto zuzugreifen. «Es ist möglich, dass unbescholtene User gesperrt werden», sagt Wenk. «Doch das nehmen wir in Kauf – besser, einmal zu viel jemanden ausschliessen als grössere Risiken zulassen.»

Weiter wird noch dieses Jahr eine Firma damit beauftragt, suspekte Aktivitäten im Edubs-Netz zu überwachen, sieben Tage die Woche und rund um die Uhr. Wenk: «Sobald die Spezialistinnen und Spezialisten etwas entdecken, das ungewöhnlich ist, isolieren sie das entsprechende System. Auch hier gilt: Lieber, ein Dienst läuft einmal nicht, als sich monatelang mit Reparieren und Reinigen herumschlagen wie nach dem Angriff im letzten Winter.»

Das ED war wohl Zufallsopfer

Zu den Kosten, welche die Attacke bislang ausgelöst hat, will sich Schenk nicht äussern. «Das können wir auch noch nicht abschliessend beziffern.» Man holte sich aber Unterstützung von Unternehmen, und das dürfte seinen Preis haben.

Hinter der Attacke auf den Basler Edubs-Server steckt mutmasslich die Hackergruppe Bian Lian. Der Kanton hat stets beteuert, es sei kein Lösegeld geflossen. Eine solche Forderung ging nur zu Beginn ein. Danach riss der Kontakt zu den Kriminellen laut Wenk aber ab: «Es kam bis heute nicht zu einer Kommunikation mit der Täterschaft.»

Das mutet seltsam an. Und deutet darauf hin, dass die Angreifer rasch merkten, dass sie es mit einem Opfer zu tun haben, bei dem finanziell kaum was zu holen ist – und sich die Mühe deshalb gar nicht lohnt.

Die IT des Kantons wurde beim Angriff auf dem falschen Fuss erwischt. Erst 2021 wurden sämtliche IT-Abteilungen des ED unter einem Dach vereinigt. Ab 2022 begann die neue IT, die Infrastruktur neu aufzubauen.

Weil jedoch etwa bei Netzwerkgeräten oder Programmen teils lange Lieferfristen bestehen, war die neue Plattform zum Zeitpunkt des Angriffs noch nicht fertig. «Das hat nun aber auch einen Vorteil», sagt Wenk. «Wir können sicher sein, dass nur die alten, anfälligeren Systeme infiziert waren, nicht die neuen.»

Das neuen Systeme soll bis Mitte 2024 vollständig zur Verfügung stehen. Teils sind neue Elemente schon in Betrieb – und können erste Erfolge verzeichnen. Kürzlich seien zwei private Geräte von Lehrpersonen durch verdächtige Aktivitäten aufgefallen, berichtet Wenk: «Wir konnten rechtzeitig reagieren, die Geräte isolieren und zusammen mit den Nutzenden reinigen.»